UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/722,423	11/28/2003	Gary Lorne MacIsaac	14534	7393

293 7590 12/12/2008
Ralph A. Dowell of DOWELL & DOWELL P.C.
2111 Eisenhower Ave
Suite 406
Alexandria, VA 22314

EXAMINER	
YUEN, KAN	

ART UNIT	PAPER NUMBER
2416	

MAIL DATE	DELIVERY MODE
12/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/722,423	MACISAAC, GARY LORNE	
	Examiner	Art Unit	
	KAN YUEN	2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on 22 August 2008.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-3,5-38,40-42 and 44-75 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-3,5-38,40-42 and 44-75 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Response to Arguments

1. Applicant's arguments, see remark, filed on 8/22/2008, with respect to the rejection(s) of claim(s) 1, 37, 38, 40 under 103 rejections have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Poletto et al. (Pub No.: 2003/0145232).

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 5, 12, 15-18, 21, 22, 37, 38, 40, 44, 49, 51, 54-56, 60, 61 are rejected under 35 U.S.C. 102(e) as being anticipated by Poletto et al. (Pub No.: 2003/0145232).

In claim 1, Poletto et al. disclosed the method of receiving a first traffic waveform representing a time distribution of data volume in a first direction in the data communication system in a first period of time; receiving a second traffic waveform representing a time distribution of data volume in a second direction in the data communication system in a second period of time (Poletto et al. see paragraphs 0007, 0092, 0095, 0102 and 0116). The attack characterization is based on comparison of historical histogram (first traffic waveform) data with near-real-time histogram (second traffic waveform); wherein an example of a histogram is shown in fig. 15A and fig. 15B. The histograms may be collected in different period of time. The gateways 26 and collectors 28 keep statistical summary information (histogram) of traffic over different periods of time and at different levels of detail. For example, a gateway 26 may keep mean and standard deviation for a chosen set of parameters across a chosen set of time-periods. The parameters may include source and destination host or network addresses, types of packets. Thus, the histograms data may be collected from different source and destination packets (different directions) in different time period;

producing a correlation value representing a correlation of the first traffic waveform with a reference waveform (Poletto et al. see paragraphs 0092, 0102). Consider a historical histogram H, and a current histogram C. Then for each bucket I component of the histogram, the noise reduction process computes a difference value D (correlation value) to determine the difference value for each bucket relative to historical norm, and produces “difference histogram” D.

producing a bandwidth anomaly signal when the correlation value satisfies a criterion (see paragraphs 0107-0112, fig. 11 and fig. 12). If the difference histogram D indicates that the most frequent packets are those with just suspicious destination addresses (bucket #4=binary 100), and those with suspicious destination addresses. Or if the indication determines that any of the parameters exceeds a particular threshold (criteria) (see paragraph 0094), the process considers this a suspicious event and begins attack characterization 139. Filtering 140 typically uses the bit vectors produced during attack characterization to decide when to drop packets, wherein by dropping the packets will decrease the overloading of upstream bandwidth caused by the attack (see paragraph 0032). In one example, the master correlation bit vector would be (00110000). Based on the broadest reasonable interpretation, the bit vector can be interpreted as the bandwidth anomaly signal.

Regarding claims 5, 44 Poletto et al. disclosed the feature of generating the first traffic waveform in response to a first set of traffic measurement values (Poletto et al. see paragraphs 0007, 0092, 0095, 0102 and 0116).

Regarding claims 12, 51Poletto et al. disclosed the feature monitoring data in the first direction and producing the first set of traffic measurement values in response thereto (Poletto et al. 0083, 0084). The gateways 26 and collectors 28 keep statistical summary information (histogram) of traffic over different periods of time and at different levels of detail. For example, a gateway 26 may keep mean and standard deviation for a chosen set of parameters across a chosen set of time-periods. The parameters may include source and destination host or network addresses, types of packets. Thus, the histograms data may be collected from different source and destination packets (different directions) in different time period;

Regarding claim 15, 54 Poletto et al. disclosed the feature wherein monitoring the data in the first direction comprises at least one of: counting packets and counting octets, in the first direction (Poletto et al. paragraphs 0037, 0038).

Regarding claims 16, 55 Poletto et al. disclosed the feature of causing a processor circuit operable to produce the first traffic waveform to communicate with at least one of a packet counter and an octet counter to receive values representing the first set of traffic measurement values (Poletto et al. paragraphs 0037, 0038).

Regarding claims 17, 56 Poletto et al. disclosed the feature of causing the processor circuit to implement at least one of the packet counter and the octet counter (Poletto et al. paragraphs 0037, 0038).

Regarding claims 18 Poletto et al. disclosed the feature of passively monitoring the data in the first direction (Poletto et al. 0083, 0084).

Regarding claims 21, 60 Poletto et al. disclosed the feature of generating the first and second traffic waveforms in response to first and second sets of traffic measurement values, representing traffic in the first and second directions on the data communication system, respectively (Poletto et al. see paragraphs 0007, 0092, 0095, 0102 and 0116).

Regarding claims 22, 61 Poletto et al. disclosed the feature wherein receiving the first and second traffic waveforms comprises receiving first and second waveforms representing first and second statistical measures of first and second time distributions respectively of data volume in first and second directions in the data communications system (Poletto et al. see paragraphs 0007, 0092, 0095, 0102 and 0116).

Claim 37, 38 and 40 are rejected similar to claim 1.

Regarding claim 49, Poletto et al. disclosed the feature wherein the processor circuit is configured to implement the first traffic waveform generator (Poletto et al. see paragraphs 0044, 0082-0084).

Claim Rejections - 35 USC § 103

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2, 3, 41, 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poletto et al. (Pub No.: 2003/0145232) in view of An (Pub No.: 2001/0040919).

For claims 2, 41 Poletto et al. did not disclose the feature wherein producing the bandwidth anomaly signal comprises producing the denial of service attack signal when the correlation value is less than a reference value. An from the same or similar fields of endeavor disclosed the feature wherein producing the bandwidth anomaly signal comprises producing the denial of service attack signal when the correlation value is less than a reference value (An see paragraph 0025, lines 1-8, and paragraph 0026, lines 1-15). The unit 126 outputs the estimated data transmission rate signal to the outside. As the result, an initial bandwidth is allocated to a device based on the estimated data rate signal. The comparison result signal can be interpreted as the DDOS signal. Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to use the method as taught by An in the network of Polette et al. The motivation for using the feature being that it provides an adjustable reference error level, so that a warning signal can be generated based on the preference of the user. Thus, it greatly increases the accuracy in the network.

Regarding claims 3, 42 An disclosed the feature of wherein producing the bandwidth anomaly signal comprises determining whether the correlation value is less than the reference value (An see paragraph 0025, lines 1-8, and paragraph 0026, lines 1-15). As shown, the unit 125 compares the value outputted from 124 with a reference error level. If the data from unit 124 is smaller than the reference error level, then the unit 125 will output the comparison result signal to unit 126.

7. Claims 6-11, 23-28, 31-34, 45-48, 50, 62-67, 70, 71, 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poletto et al. (Pub No.: 2003/0145232) in view of Berkner et al. (Pub No.: 2007/0160304).

For claims 6, 45 Poletto et al. did not disclose the feature wherein generating the first traffic waveform comprises subjecting the first set of traffic measurement values to a Discrete Wavelet Transform. Berkner et al. from the same or similar fields of endeavor disclose the feature wherein generating the first traffic waveform comprises subjecting the first set of traffic measurement values to a Discrete Wavelet Transform (Berkner et al. paragraph 157). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to use the method as taught by Berkner et al. in the network of Polette et al. The motivation for using the feature being that it removes quantization noise, thus it reduces transmission packet error rate in the network.

Regarding claims 7, 46 Berkner et al. disclosed the feature wherein subjecting the first set of traffic measurement values to the Discrete Wavelet Transform comprises using Haar wavelet filter coefficients in the Discrete Wavelet Transform (Berkner et al. paragraph 157).

Regarding claims 8, 47 Berkner et al. disclosed the feature wherein generating the first traffic waveform comprises causing the Discrete Wavelet Transform to produce a first component, the first component representing the first traffic waveform (Berkner et al. paragraph 157).

Regarding claims 9, 48 Poletto et al. wherein producing the correlation value comprises correlating the first component with the reference waveform (Poletto et al. see paragraphs 0092, 0102).

Regarding claim 10, Poletto et al. disclosed the feature of using a processor circuit to generate the first traffic waveform and to correlate the first traffic waveform with the reference waveform (Poletto et al. see paragraphs 0092, 0102).

Regarding claims 11, 50 Poletto et al. disclosed the feature wherein the first traffic waveform represents a statistical measure of a time distribution of data volume in the first direction (Poletto et al. see paragraphs 0007, 0092, 0095, 0102 and 0116)

Regarding claims 23, 62 Berkner et al. disclosed the feature of subjecting the first and second sets of traffic measurement values respectively, to a Discrete Wavelet Transform (Berkner et al. paragraph 157).

Regarding claims 24, 63 Berkner et al. disclosed the feature of using Haar wavelet filter coefficients in the Discrete Wavelet Transform (Berkner et al. paragraph 157).

Regarding claims 25, 64 Berkner et al. disclosed the feature causing the Discrete Wavelet Transform to produce a first component, representing the first traffic waveform and a second component representing the second traffic waveform (Berkner et al. paragraph 157).

Regarding claims 26, 65 Poletto et al. disclosed the feature wherein producing the correlation value comprises correlating the first and second components (Poletto et al. see paragraphs 0092, 0102).

Regarding claims 27, 66 Poletto et al. disclosed the feature of implementing a traffic waveform generator in a processor circuit used to produce the correlation value (Poletto et al. see paragraphs 0092, 0102).

Regarding claims 28, 67 Poletto et al. disclosed the feature of monitoring data in the first and second directions and producing the first and second sets of traffic measurement values respectively in response thereto (Poletto et al. 0083, 0084). The gateways 26 and collectors 28 keep statistical summary information (histogram) of traffic over different periods of time and at different levels of detail. For example, a gateway 26 may keep mean and standard deviation for a chosen set of parameters across a chosen set of time-periods. The parameters may include source and destination host or network addresses, types of packets. Thus, the histograms data may be collected from different source and destination packets (different directions) in different time period;

Regarding claims 31, 70 Poletto et al. disclosed the feature wherein monitoring the data comprises at least one of: packet counters and octet counters in each of the first and second directions (Poletto et al. paragraphs 0037, 0038).

Regarding claim 32, Poletto et al. disclosed the feature of comprising causing a processor circuit operable to produce the first and second traffic waveforms to communicate with at least one of a packet counter and an octet counter to receive values representing the first and second sets of traffic measurement values (Poletto et al. paragraphs 0037, 0038).

Regarding claim 33, Poletto et al. disclosed the feature of causing the processor circuit to implement at least one of the packet counter and the octet counter (Poletto et al. paragraphs 0037, 0038).

Regarding claim 34, Poletto et al. disclosed the feature of passively monitoring the data in the first and second directions (Poletto et al. 0083, 0084).

Regarding claim 71, Poletto et al. disclosed the feature wherein the processor circuit is configured to communicate with the communication interface to receive values produced by at least one of the packet counter and the octet counter, the values representing the first and second sets of traffic measurement values (Poletto et al. see paragraphs 0007, 0092, 0095, 0102 and 0116). The gateways 26 and collectors 28 keep statistical summary information (histogram) of traffic over different periods of time and at different levels of detail. For example, a gateway 26 may keep mean and standard deviation for a chosen set of parameters across a chosen set of time-periods. The parameters may include source and destination host or network addresses, types of packets. Thus, the histograms data may be collected from different source and destination packets (different directions) in different time period;

Regarding claim 72, Poletto et al. disclosed the feature wherein the processor circuit is configured to implement the communication interface (Poletto et al. see paragraphs 0044, 0082-0084).

8. Claims 13, 14, 29, 30, 52, 53, 68, 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poletto et al. (Pub No.: 2003/0145232) in view of Berkner et al. (Pub No.: 2007/0160304) as applied to claim 12above, and further in view of Chen et al. (Pub No.: 2004/0017779).

For claims 13, 52 Poletto et al. and Berkner et al. both did not disclose the feature wherein producing the first set of traffic measurement values comprises producing values representing a property of an Ethernet statistics group in a remote monitoring protocol. Chen et al. from the same or similar fields of endeavor disclosed the feature wherein producing the first set of traffic measurement values comprises producing values representing a property of an Ethernet statistics group in a remote monitoring protocol (Chen et al. see paragraph 0002, lines 1-7). The Ethernet switch monitors remote equipment and to drive a warning message email message to remote equipment. The Ethernet switch can be the Ethernet statistics group, and the email is the remote monitoring protocol. Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to use the method as taught by Chen et al. in the network of Poletto et al. and Berkner et al. The motivation for using the feature being that it provides system security.

Regarding claims 14, 53 Chen et al. disclosed the feature of causing a processor circuit operable to produce the first traffic waveform to communicate with a communication interface to receive the values representing the property of an Ethernet statistics group (Chen et al. see paragraph 0002, lines 1-7).

Regarding claims 29, 68 Chen et al. disclosed the feature of wherein producing the first and second sets of traffic measurement values comprises producing values representing a property of an Ethernet statistics group in a remote monitoring protocol, for each of the first and second directions (Chen et al. see paragraph 0002, lines 1-7). The Ethernet switch monitors remote equipment and to drive a warning message email message to remote equipment. The Ethernet switch can be the Ethernet statistics group, and the email is the remote monitoring protocol.

Regarding claims 30, 69 Chen et al. disclosed the feature of causing a processor circuit operable to produce the first and second traffic waveforms to communicate with a communication interface to receive the values representing a property of an Ethernet statistics group (Chen et al. see paragraph 0002, lines 1-7). The Ethernet switch monitors remote equipment and to drive a warning message email message to remote equipment. The Ethernet switch can be the Ethernet statistics group, and the email is the remote monitoring protocol.

9. Claims 19, 20, 35, 36, 58, 59, 74, 75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poletto et al. (Pub No.: 2003/0145232) in view of D'souza et al. (Pat No.: 6704289).

For claims 19, 58 Poletto et al. did not disclose the feature of signaling an operator in response to the bandwidth anomaly signal. D'souza et al. from the same or similar fields of endeavor disclosed the feature signaling an operator in response to the bandwidth anomaly signal (D'souza et al. column 3, lines 45-67, column 4, lines 1-45, fig. 3). Upon determining the route cause, the event correlation mechanism 212 signals a trouble ticket system 218 to generate a trouble ticket 220 to notify network operations personnel to restore customer bandwidth by way of repair adjustment, modification or enhancement to the network. Thus, the trouble ticket is the bandwidth anomaly signal.

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to use the method as taught by D'souza et al. in the network of Poletto et al. The motivation for using the feature being that it reduces system resources.

Regarding claims 20, 59 D'souza et al. disclosed the feature of controlling at least one of transmission and reception of data from the data communication system in response to the bandwidth anomaly signal (D'souza et al. column 3, lines 45-67, column

4, lines 1-45, fig. 3). Upon determining the route cause, the event correlation mechanism 212 signals a trouble ticket system 218 to generate a trouble ticket 220 to notify network operations personnel to restore customer bandwidth by way of repair adjustment, modification or enhancement to the network. Thus, the trouble ticket is the bandwidth anomaly signal.

Regarding claims 35, 74 D'souza et al. disclosed the feature of transmitting and receiving data from a data communication system, the data communication method of claim 1 and further comprising signaling an operator in response to the bandwidth anomaly signal (D'souza et al. column 3, lines 45-67, column 4, lines 1-45, fig. 3). Upon determining the route cause, the event correlation mechanism 212 signals a trouble ticket system 218 to generate a trouble ticket 220 to notify network operations personnel to restore customer bandwidth by way of repair adjustment, modification or enhancement to the network. Thus, the trouble ticket is the bandwidth anomaly signal.

Regarding claims 36, 75 D'souza et al. disclosed the feature of transmitting and receiving data from a data communication system, the data communication method of claim 1 and further comprising controlling at least one of the transmission and reception of data from the data communication system in response to the bandwidth anomaly signal (D'souza et al. column 3, lines 45-67, column 4, lines 1-45, fig. 3). Upon determining the route cause, the event correlation mechanism 212 signals a trouble ticket system 218 to generate a trouble ticket 220 to notify network operations personnel to restore customer bandwidth by way of repair adjustment, modification or enhancement to the network. Thus, the trouble ticket is the bandwidth anomaly signal.

10. Claims 57, 73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poletto et al. (Pub No.: 2003/0145232) in view of Ramakrishnan (Pub No.: 2003/0012196).

For claims 57, 73 Poletto et al. did not disclose the feature of a passive monitor operable to passively monitor the data in the first direction and to provide a copy of the data in the first direction to the communication interface. Ramakrishnan from the same or similar fields of endeavor disclosed the feature of a passive monitor operable to passively monitor the data in the first direction and to provide a copy of the data in the first direction to the communication interface (Ramakrishnan see paragraph 0009). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention to use the feature as taught by Ramakrishnan. The motivation for using the feature being that it provides a historical data log for future measurement utilization and thus it increases system adaptability.

Examiner's Note:

Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAN YUEN whose telephone number is (571)270-1413. The examiner can normally be reached on Monday-Friday 10:00a.m-3:00p.m EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Ricky O. Ngo can be reached on 571-272-3139. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kan Yuen/
Examiner, Art Unit 2416

/Ricky Ngo/
Supervisory Patent Examiner, Art Unit 2416

KY